Global Roaming Trust-based Model for V2X Communications

Aljawharah Alnasser
Department of Information Technology
King Saud University
Riyadh, Saudi Arabia
alalnasser@ksu.edu.sa

Hongjian Sun
Department of Engineering
Durham University
Durham, UK
hongjian.sun@durham.ac.uk

***Abstract*—Smart cities need to connect physical devices as a network to improve the efficiency of city operations and services. Intelligent Transportation System (ITS) is a key component of smart cities. ITS supports the communication between vehicles to improve the driving experience and achieve active transportation. The communication is provided using Vehicle-to-Everything (V2X) communication technology. Cyber-security is currently one of the main challenges facing V2X technology. A V2X communication link is vulnerable to various cyber-attacks including internal and external attacks. Internal attacks cannot be detected by traditional security schemes because the compromised nodes have valid credentials. Thus, a trust model is needed to defend against them. In this paper, a global roaming trust-based security model is proposed for V2X communication. Each vehicle has a global knowledge about malicious nodes in the network. In addition, we conduct various experiments with different percentage of malicious nodes to measure the performance of the proposed model. Simulation results show that the proposed model improves False Negative Rate (FNR) by 33.5% in comparison with the existing model.**

***Index Terms*—Trust, V2X, Malicious, Vehicle.**

I. Introduction

Intelligent Transportation System (ITS) is one of the leading smart systems which have been developed to obtain reliable transportation. Each vehicle can establish a communication with other vehicles and infrastructure units using Vehicle-to-Everything (V2X) communications. Vehicles include all moving road entities such as cars, bicycles, buses, trains and motorcycles. Each road entity periodically broadcasts a message which contains status information such as speed, directions and location. V2X supports several types of communication links as shown in Fig.1, e.g. Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), Vehicle-to-Grid (V2G) and Vehicle-to-Infrastructure (V2I).

As a consequence, the communication link between road entities is exposed to either internal or external cyber-attacks. *External attacks* means unauthorized nodes launch the malicious behavior. However, the network can be protected against these attacks by applying traditional security schemes such as encryption and authentication. *Internal attacks* means authorized nodes initiate the malicious behavior. The compromised nodes are hard to be detected because they have valid credentials. As a result, a trust-based model was suggested to protect the network against internal attacks [1]. It is based on continuous monitoring for the surrounding nodes' behavior. When a misbehavior node is detected, a warning alarm is sent throughout the network [2].

A. Alnasser is also with School of Engineering and Computing Sciences, Durham University, Durham.

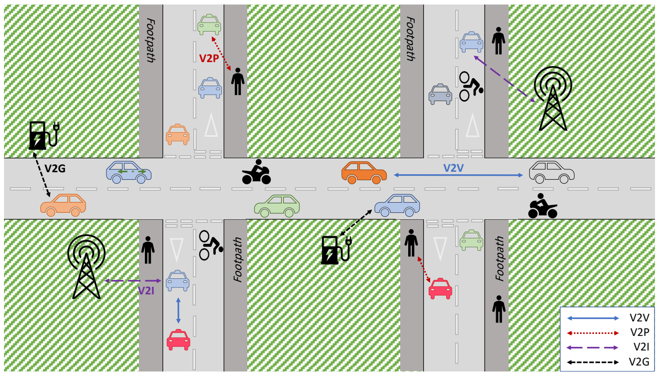


Fig. 1. V2X communication links

Recent research focus on developing security models that provide data confidentiality in V2X communications. For instance, Liu *et al.* [3] designed a privacy-preserving ad conversion protocol for V2X-assisted proximity marketing that achieves input certification and output verifiability against malicious ad networks. Also, Ulybyshev *et al.* [4] suggested a data exchange method for V2X communication systems, which provides data confidentiality and integrity. The method supports encrypted search over encrypted vehicle records that could be stored in untrusted cloud. In addition, Simplicio *et al.* [5] improved the structure of SCMS's certificate revocation and linkage approach by addressing some limitations. The proposed modifications support the temporary revocation and linkage of pseudonym certificates. Furthermore, Cheng *et al.* [6] presented a remote attestation security model based on a privacy-preserving blockchain. The model is comprised of two main parts. The first is identity authentication; and the second is the calculation of the nodes to make final decisions and write them into data blocks.

Moreover, various security models have been suggested to ensure the authentication in V2X networks. For instance, Yang *et al.* [7] implemented an authentication model for V2X communications. The model consists of two schemes for various communication types. One scheme was designed for V2V communication, while the other was suggested for V2I communication. Also, Villarreal-Vasquez *et al.* [8] proposed a dynamic approach which achieves the trade-off between safety, security and performance of V2X systems. However, the analysis is concentrated on V2V communications which are compliant with IEEE802.11p. In addition, Kiening *et al.* [9] studied the security requirements for V2X systems to design Trust Assurance Levels (TAL). They designed a certification framework to support trust establishment between road entities in V2X communication. Indeed, the node is trusted when it is correctly authenticated. Also, Ahmed and Lee [10] performed an evaluation for the security services of the new LTE-based V2X architecture. Based on their evaluation results, they proposed a practical solution to provide privacy and achieve basic security requirements of message exchange in V2X network. Also, Jung *et al.* [11] suggested a procedure and test scenario to achieve secure communication for autonomous cooperation driving. The procedure is configured according to the following phases: issuing certificates, key and certificate installation and secure communication. On the other hand, some research provide a solution for data integrity. The proposed model in [12] considered the security in sensing systems for V2X networks because the vehicular network relies on sensor information to achieve safe traffic. It was developed to defend against both false data injection and packet drop attacks. All these solutions can protect the network against external attacks only. However, the vehicular network should also be safeguarded against internal attacks.

To overcome these limitations, this paper proposes a global roaming trust-based model for V2X communications. We evaluate the performance of the proposed model by comparing it with an existing model [13]. The simulation results show that the proposed model outperforms the existing one. This paper makes two main contributions to the field of vehicular network security:

- This paper proposes a global roaming trust-based model for V2X communication. Different from existing research, the nodes have global knowledge about malicious nodes in the network.
- This paper compares the performance of the proposed model with the exsiting model in [13]; our model improves the False Negative Rate (FNR) with 33.5% when the percentage of malicious nodes is around 87.5%.

The paper is organised as follows: in section II we describe the proposed system model. In section III we present a detailed description of the proposed trust model. In section IV we present the simulation setup parameters and conduct various experiments to measure the model performance. In section V we evaluate the proposed model by comparing it with the existing model [13]. Finally, Section VI concludes the overall work.

II. Proposed System Model

The considered network consists of N road entities, which move at various speeds, and M fixed Road Side Units (RSUs). Each road entity sends three types of messages: *Beacon message* which is sent periodically to inform the surrounding nodes about its current speed, location and direction; *transaction message* which contains confidential information and it is sent to the core network; and *warning message* that is sent to the surrounding RSUs when a malicious node is detected. Each time the road entity sends a message to the core network, it should go through the following phases:

- *Connectivity phase:* each road entity examines its connectivity with the core network and the surrounding entities.
- *Communication phase:* if the source entity has a connection with the core network, it forwards its packet to the nearest RSU. Otherwise, the packet is sent to a trusted entity to relay them to the core network.

Moreover, the considered network has two types of nodes which are normal and malicious nodes. The normal node keeps monitoring the surrounding environment and sends its packets to the core network. Also, it relays any received packet to the nearest RSU. On the other hand, the malicious node launches various attacks to disturb the network performance such as:

- Selective forwarding attack: occurs when the malicious node drops some of the received packets randomly to escape punishment.
- Recommendation attacks: happens when the malicious node sends bogus recommendations regarding other nodes as follows:
  - In good-mouthing attack, the malicious node f sends good recommendations regarding other malicious nodes $h_1, h_2, ...\ h_{np}$ as shown in Fig.2(a). In this attack, the malicious nodes h could be considered as normal nodes. Thus, the malicious node f disturbs the decision phase.
  - In bad-mouthing attack, the malicious node f sends bad recommendations regarding other normal nodes $q_1, q_2, ...\ q_{np}$ as shown in Fig.2(b). In this attack, the normal nodes q may be classified by node i as malicious nodes.

III. Global Roaming Trust-based Model

The global roaming trust-based model maintains two levels of trust as shown in Fig.3: *road entity level* and *RSU level*. Each road entity evaluates the trustworthiness of the surrounding entities. Then, it sends warning messages to the surrounding RSUs when a malicious node is detected. When the RSUs receive high volume of warning messages from the surrounding entities, they generate an alarm and send it to the central unit. In this section, we will describe the proposed model in details.

A. Road entity level

During time interval t, each road entity measures the trustworthiness of all surrounding entities. Indeed, node i

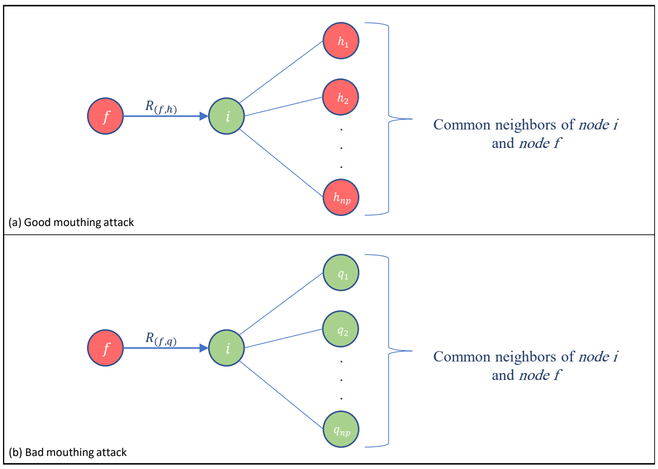


Fig. 2. General model for recommendation attacks

continuously monitors its one-hop neighbors j. Then, node i is able to compute direct trust using the collected information. In addition, node i sends recommendation requests to the surrounding nodes k regarding node j. The proposed model manages two trust components as follows.

- **Current Trust** - $T^{(t)}_{current(i,j)}$: it is computed by node i to evaluate the communication experience with node j during time interval t. It is calculated using

$$T^{(t)}_{current(i,j)} = \frac{T^{(t)}_{past(i,j)} + T^{(t)}_{direct(i,j)}}{2} \tag{1}$$

It is measured based on the following trust values:

  - *Past trust* - $T^{(t)}_{past(i,j)}$: it is a measure for the past behavior of node j. The past trust is considered to prevent the non-continuous malicious behavior.
  - *Direct trust* - $T^{(t)}_{direct(i,j)}$: it is an evaluation for the communication experience with the neighboring nodes j. It is computed using

$$T^{(t)}_{direct(i,j)} = \frac{Successful\_Interactions}{Total\_Interactions} \tag{2}$$

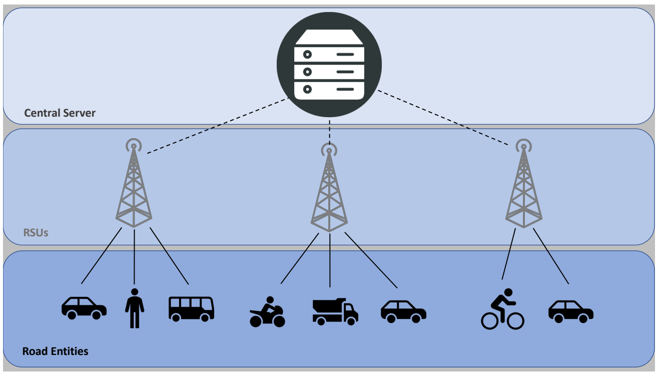


Fig. 3. Trust levels in the proposed model

where $Successful\_Interactions$ is the number of successful interactions between node i and node j, and $Total\_Interactions$ is the total number of interactions between node i and node j.

- **Indirect Trust** - $T^{(t)}_{indirect(i,j)}$: it is a measure for the behavior of the neighboring nodes j using the surrounding nodes' opinions. Indeed, node i collects recommendations from the surrounding nodes regarding node j. Before computing indirect trust, node i applies the following steps:
  - *Confidence value computation*- $C^{(t)}_{(i,k)}$: node i measures the confidence value for each recommender node k. $C^{(t)}_{(i,k)}$ is computed by

$$C^{(t)}_{(i,k)} = \begin{cases} 1, & \text{if } T^{(t)}_{l(i,k)} \geq Th_{max}. \\ C_w, & \text{if } Th_{min} \leq T^{(t)}_{l(i,k)} < Th_{max}. \\ 0, & \text{if } T^{(t)}_{l(i,k)} < Th_{min}. \end{cases} \tag{3}$$

  where C_w is the confidence weight for uncertain recommendations.
  - *Recommendations clustering*: node i classifies the received recommendations into two groups which

TABLE I
LOCAL TRUST COMPUTATION OF THE PROPOSED MODEL

	Existing of current communication between node i and node j	Existence of the recommendations about node j	w_1	$Trust_1$	w_2	$Trust_2$
First time communication	✓	✓	Eq.(7)	$T^{(t)}_{indirect(i,j)}$	$1-w_1$	$T^{(t)}_{direct(i,j)}$
	✓	✗	1	$T^{(t)}_{direct(i,j)}$	0	–
	✗	✓	1	$T^{(t)}_{indirect(i,j)}$	0	–
	✗	✗	1	$T^{(0)}_{l(i,j)}$	0	–
Have Previous Communication	✓	✓	Eq.(7)	$T^{(t)}_{indirect(i,j)}$	$1-w_1$	$T^{(t)}_{current(i,j)}$
	✓	✗	1	$T^{(t)}_{current(i,j)}$	0	-
	✗	✓	Eq.(7)	$T^{(t)}_{indirect(i,j)}$	$1-w_1$	$T^{(t)}_{past(i,j)}$
	✗	✗	1	$T^{(t)}_{past(i,j)}$	0	–

are positive and negative recommendations using Th_{min}.

After that, each node i calculates indirect trust for node j by applying different weights α and β for $P_{(i,j)}^{(t)}$ and $N_{(i,j)}^{(t)}$ respectively. It is calculated using

$$T_{indirect(i,j)}^{(t)} = \alpha \times P_{(i,j)}^{(t)} + \beta \times N_{(i,j)}^{(t)} \tag{4}$$

where $P_{(i,j)}^{(t)}$ is the average value of positive recommendations; and $N_{(i,j)}^{(t)}$ the average value of negative recommendations. The weights are computed by

$$\alpha = \frac{n}{n+m}, \beta = \frac{m}{n+m} \tag{5}$$

where n and m are the number of positive and negative recommendations respectively.

- **Local Trust -** $T_{l(i,j)}^{(t)}$: each node i is able to compute local trust for node j and make a decision. Generally, local trust is computed using

$$T_{l(i,j)}^{(t)} = w_1 \times Trust_1 + w_2 \times Trust_2 \tag{6}$$

where $Trust_1$ and $Trust_2$ are adjusted based on three factors which are the occurrence of current communications between node i and node j; the existence of the recommendations about node j; and the presence of a previous connection between node i and node j. The measurement of $Trust_1$ and $Trust_2$ are described in Table I.

In addition, trust weights w_1 and w_2 are changed based on recommendation factor (RC) and the number of neighbors. w_1 and w_2 are weights for indirect trust and (direct/current or past) trust respectively. w_1 represents the recommendation rate as follows:

$$w_1 = (m+n) \times \frac{RC}{Neighbors^{(t)}} \tag{7}$$

where $w_2 = 1 - w_1$, and $Neighbors^{(t)}$ is the number of node i neighbors at time t.

- **Local decision**: each node i has a local blacklist which has a list of malicious nodes based on the local decision. Thus, node i stops the communication with any node j in the blacklist. The decision is made using

$$D_{Local} = \begin{cases} Trusted, & \text{if } T_{l(i,j)}^{(t)} \geq Th_{max}. \\ Uncertain, & \text{if } Th_{min} \leq T_{l(i,j)}^{(t)} < Th_{max}. \\ Malicious, & \text{if } T_{l(i,j)}^{(t)} < Th_{min}. \end{cases} \tag{8}$$

where Th_{min} and Th_{max} are minimum and maximum trust thresholds respectively. When trust value exist between them, the node is classified as uncertain node. After that, the node updates its local blacklist and sends malicious and uncertain warning messages to the surrounding RSUs.

B. RSU level

During time interval t', where $t' > t$, RSUs start trust calculation phase. First, each RSU measures the percentage of malicious and uncertain alarms regarding node j using

$$M = \frac{m'}{t'}, \qquad U = \frac{u}{t'} \tag{9}$$

where m' and u are the number of malicious and uncertain warnings respectively. Second, each RSU is able to make a decision regarding node j using

$$Decision_j = Rate_M - Rate_U \tag{10}$$

where $Rate_M$ and $Rate_U$ are the rates of malicious alarms and uncertain alarms respectively. They are calculated using

$$Rate_M = \frac{M}{M+U} \tag{11}$$

$$Rate_U = \frac{U}{M+U} \tag{12}$$

Finally, the RSU classifies node j as malicious node when $Decision_j > 0$. Therefore, RSU sends malicious alarm to the central server.

C. Global Trust decision

At this stage, central server can make global decision regarding node j based on the alarms which are received from RSUs.

$$D_{Global} = \begin{cases} Malicious, & \text{if } A_m \geq \frac{Total\_RSUs}{2} - 1. \\ Normal, & \text{Otherwise.} \end{cases} \tag{13}$$

where A_m is the number of malicious warnings that are received regarding node j. Node j is added to the global blacklist when it is classified as malicious node. Central server broadcasts the updated global blacklist to RSUs. Then, RSUs rebroadcast it again to all roads entities that are covered by the network. The road entities updates the local blacklist based on the received global blacklist.

IV. Simulation Analysis

This section describes the simulation setup used to measure and evaluate the performance of the proposed model. In addition, we analyse the effect of various parameters on the false alarm rate.

A. Network specifications

In our simulations, we considered a V2X network with 24 road entities and 9 RSUs with parameters as shown in Table II. The road entities move over an area of 900×900 m^2 with various speed ranges. The road entity sends the transaction message to the core network directly or using a multi-hop routing protocol.

To measure the performance of the proposed trust model, we study various types of malicious nodes: six selective forwarding attackers, three good-mouthing attackers and three bad-mouthing attackers.

TABLE II
SIMULATION PARAMETERS

Parameter	Value
Simulation time (T)	100 iteration
Speed ranges	Vehicle:(10-30) m/s, Pedestrians:(0-8) m/s Cycles:(3-10) m/s, Motorcycle:(10-30) m/s
Number of nodes	24 nodes
Th_{max}	0.7
Th_{min}	0.4
RC	0.3
C_w	0.9
$T^{(0)}_{l(i,j)}$	0.5

B. Results

In this section, we study the impact of changing various parameters on the global trust measure and relate these to the false alarm rate. False alarm rate includes False Negative Rate (FNR) and False Positive Rate (FPR). FNR measures the rate of undetected attacks, while, FPR measures the rate of classifying normal nodes as malicious. In addition, we start the simulation using the initial parameters which are $Th_{max} = 0.9; RC = 0.3; C_w = 0.9$. Then, we update their values with the optimal onces.

1) Effect of trust thresholds on false alarm rate: The simulation experiments were run with initial parameters. We study how various values of Th_{min} has an impact on false alarm rate. Also, it helps us to define the optimal value for Th_{min}. The corresponding results are shown in Fig.4 (a). The following remarks can be made:

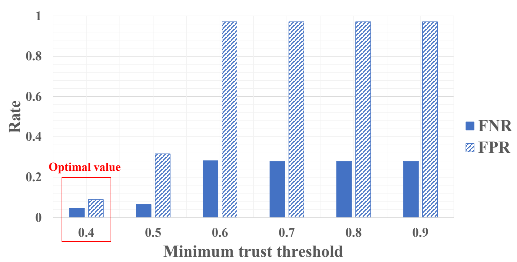
- FNR increases when the value of Th_{min} increases;
- FPR rises significantly as long as the Th_{min} increases;
- the impact of Th_{min} is high on FPR because as long as Th_{min} goes up that means the malicious range is expanded. As a result, many normal nodes are classified as malicious nodes;
- we found that when $Th_{min} = 0.4$, it achieves low FNR and FPR values.

Moreover, we study how various values of Th_{max} has an impact on false alarm rate. The experiment was run with initial parameters and $Th_{min} = 0.4$. The corresponding results are shown in Fig.4 (b). We notice that FNR slightly decreases when the value of Th_{max} increases, however, the FPR slightly goes up as long as the Th_{max} increases. We update initial value of Th_{max} with 0.7 which is the optimal value.

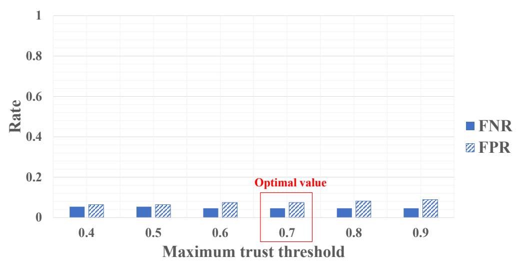
2) Effect of recommendation factor (RC): The simulation experiments were run with updated initial parameters. Here, we study the effect of various values of RC on the false alarm rate. By inspecting Fig.5 (a), the following remarks can be made:

- FPR goes up when the value of RC increases to reach approximately 0.27, however, the FNR is stable while RC increases;
- the RC has an impact on FPR only because RC is a part of the calculation of indirect trust weight w_1. Therefore, giving high weight to indirect trust results high FPR. As a result, the model starts making false decisions regarding the normal nodes.
- we choose $RC = 0.3$ as an optimal value which is the same as initial value.

3) Effect of Confidence weight (C_w): We examine various values of C_w to choose the value that achieves minimum false

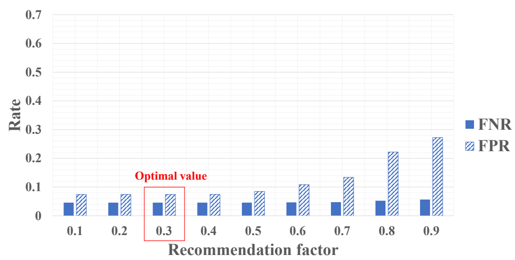


(a) Minimum threshold (Th_{min})

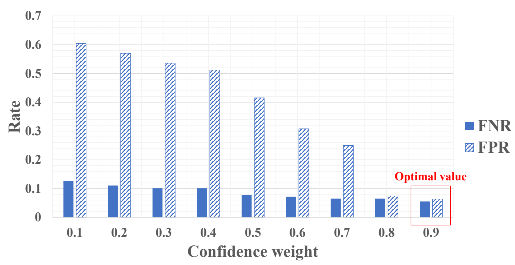


(b) Maximum threshold (Th_{max})

Fig. 4. Effect of changing trust thresholds on false alarm rate



(a) Recommendation factor (RC) in eq.(7)



(b) Confidence weight (C_w) in eq.(3)

Fig. 5. Effect of changing Recommendation factor and confidence weight on false alarm rate

alarm rate. The corresponding results are shown in Fig.5 (b). We notice the following:

- FPR goes down when the C_w increases because we give lower weight for the recommendations that are sent by uncertain nodes, however, the FNR decreases slightly when the C_w increases;
- we notice that the most of normal nodes is classified as uncertain nodes, thus, giving their recommendations low weight results high FPR.
- we found out that the initial value of C_w is the optimal one.

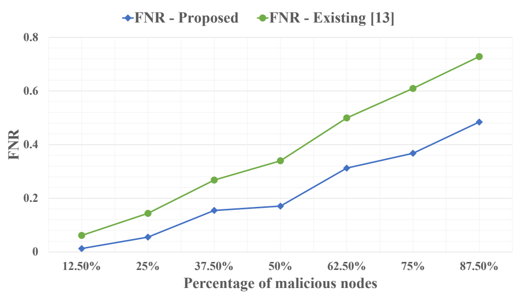
V. Performance Evaluation

We use the existing model in [13] as a benchmark to evaluate the performance of the proposed model. The impact of various rates of malicious nodes on the false alarm rate is studied on the proposed model and existing model.

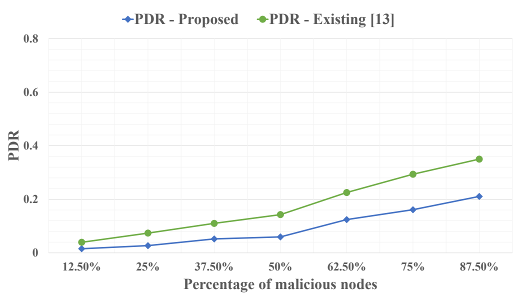
A. *Effect of selective forwarding attack on FNR*

Generally, when the model has a low FNR, it is able to detect the most malicious nodes. The result that is shown in Fig.6 (a) represents the FNR for various percentages of malicious nodes. The following remarks can be made:

- in the existing model, the FNR reaches to 0.73 when the percentage of malicious nodes is equal to 87.50%.
- FNR values in the proposed model is reduced. Thus, the global decision has the minimum FNR value for all rates of malicious nodes.



(a) FNR



(b) PDR

Fig. 6. Effect of selective forwarding attack on FNR and PDR

B. *Effect of selective forwarding attack on PDR*

To measure the model performance, we measure the PDR with different percentage of malicious nodes as shown in Fig.6 (b). Generally, the PDR is increasing when the percentage of malicious nodes is increasing. In addition, the existing model produces high PDR which results from the high FNR. On the other hand, the proposed model has lower PDR which improves the network performance.

C. *Measuring the improvement rate*

We measure the improvement rate on FNR and PDR for the proposed model in comparison with the existing model [13] as shown in Fig.7. We notice that the FNR is highly improved in the proposed model when the percentage of malicious nodes is equal to 12.50%. In addition, the rate at 50%, which is a high percentage, increases again to around 50%.

Moreover, we notice that the proposed model provides high improvement on PDR in comparison with the existing model, thus, it gains better network performance.

VI. Conclusion

In this paper, we proposed a global roaming trust-based model for the V2X network. Various malicious behaviors are considered to study the performance of the proposed model which are selective forwarding attack, bad-mouthing attack and good-mouthing attack. We conducted various experiments with different percentage of malicious nodes. Comparison results showed that the proposed model improved FNR by 33.5% and PDR by 40% when the percentage of malicious nodes is equal to 87.50%.

In future work, we will improve the proposed model to consider RSU attacks.

References

[1] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[2] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, 2016.

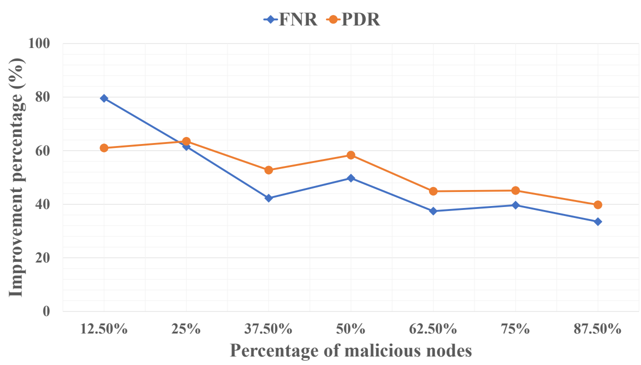


Fig. 7. Improvement rate on FPR and PDR in the proposed model

[3] D. Liu, J. Ni, H. Li, X. Lin, and X. Shen, “Efficient and privacy-preserving ad conversion for v2x-assisted proximity marketing,” in *Proc. IEEE 15th Int. Conf. Mobile Ad Hoc and Sensor Systems (MASS)*, Oct. 2018, pp. 10–18.

[4] D. Ulybyshev, A. O. Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. B. Othmane, “Secure data communication in autonomous v2x systems,” in *Proc. IEEE Int. Congress Internet of Things (ICIOT)*, Jul. 2018, pp. 156–163.

[5] M. A. S. Junior, E. L. Cominetti, H. K. Patil, J. Ricardini, L. Ferraz, and M. V. Silva, “Privacy-preserving method for temporarily linking/revoking pseudonym certificates in vanets,” in *Proc. Security And Privacy In Computing And Communications/ 12th IEEE Int 2018 17th IEEE Int. Conf. On Trust Conf. On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2018, pp. 1322–1329.

[6] C. Xu, H. Liu, P. Li, and P. Wang, “A remote attestation security model based on privacy-preserving blockchain for v2x,” *IEEE Access*, vol. 6, pp. 67 809–67 818, 2018.

[7] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, “V2X security: A case study of anonymous authentication,” *Pervasive and Mobile Computing*, 2017.

[8] M. Villarreal-Vasquez, B. Bhargava, and P. Angin, “Adaptable safety and security in v2x systems,” in *Proc. IEEE Int. Congress Internet of Things (ICIOT)*, Jun. 2017, pp. 17–24.

[9] A. Kiening, D. Angermeier, H. Seudie, T. Stodart, and M. Wolf, “Trust assurance levels of cybercars in v2x communication,” in *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*, ser. CyCAR ’13. New York, NY, USA: ACM, 2013, pp. 49–60. [Online]. Available: http://doi.acm.org/10.1145/2517968.2517974

[10] K. J. Ahmed and M. J. Lee, “Secure, lte-based v2x service,” *IEEE Internet of Things Journal*, 2017.

[11] H. Jung, K. Lim, D. Shin, S. Yoon, S. Jin, S. Jang, and J. Kwak, “Reliability verification procedure of secured v2x communication for autonomous cooperation driving,” in *Proc. Int. Conf. Information and Communication Technology Convergence (ICTC)*, Oct. 2018, pp. 1356–1360.

[12] A. Chattopadhyay, U. Mitra, and E. G. StrÃűm, “Secure estimation in v2x networks with injection and packet drop attacks,” in *Proc. 15th Int. Symp. Wireless Communication Systems (ISWCS)*, Aug. 2018, pp. 1–6.

[13] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, “Recommendation based trust model with an effective defence scheme for MANETs,” *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101–2115, 2015.